日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１２月　９日

出願番号
Application Number:　特願２００２－３５６５１５

[ST.10/C]:　[ＪＰ２００２－３５６５１５]

出願人
Applicant(s):　コナミ株式会社

２００３年　６月２５日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０５０２０６

【書類名】　特許願
【整理番号】　P1729
【提出日】　平成14年12月 9日
【あて先】　特許庁長官殿
【国際特許分類】　A63F 13/00
A63F 13/10
【発明者】
【住所又は居所】　東京都港区芝四丁目１番２３号　株式会社コナミコンピュータエンタテインメントスタジオ内
【氏名】　森　昌二
【特許出願人】
【識別番号】　000105637
【氏名又は名称】　コナミ株式会社
【代理人】
【識別番号】　100107331
【弁理士】
【氏名又は名称】　中村　聡延
【電話番号】　03-5524-2323
【選任した代理人】
【識別番号】　100099645
【弁理士】
【氏名又は名称】　山本　晃司
【電話番号】　03-5524-2323
【選任した代理人】
【識別番号】　100108800
【弁理士】
【氏名又は名称】　星野　哲郎
【電話番号】　03-5524-2323

【先の出願に基づく優先権主張】

【出願番号】　特願2002-272794

【出願日】　平成14年 9月19日

【手数料の表示】

【予納台帳番号】　131957

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0110288

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証処理ハードウェア、認証処理システム、及び、利用管理ハードウェア

【特許請求の範囲】

【請求項１】　ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアであって、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備えることを特徴とする認証処理ハードウェア。

【請求項２】　前記復号化処理部は、１つの前記暗号鍵を利用した復号化処理を１回に限り行うことを特徴とする請求項１に記載の認証処理ハードウェア。

【請求項３】　前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備えることを特徴とする請求項１又は２に記載の認証処理ハードウェア。

【請求項４】　ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行するハードウェアと、を備える認証処理システムであって、

前記サーバ装置は、

前記ハードウェアからの認証要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する暗号鍵送信部と、

前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備え、

前記ハードウェアは、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備え、

前記端末装置は、

前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、

前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備えることを特徴とする認証処理システム。

【請求項５】　端末装置に取り付けられ、前記端末装置の利用可否の管理処理を実行する利用管理ハードウェアであって、

前記端末装置の利用可否を示す利用可否情報を記憶する記憶部と、

前記端末装置から、動作要求を受信する受信部と、

前記利用可否情報に基づいて前記端末装置の利用可否を判定する判定部と、

前記端末装置の利用が可能であると前記判定部が判定したときに、前記端末装置を動作可能とする制御部と、を備えることを特徴とする利用管理ハードウェア

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークゲームにおけるユーザ認証、利用期間管理などを含むセキュリティ管理手法に関する。

【０００２】

【従来の技術】

近年では、家庭用ゲーム機などの端末装置でインターネットなどを介してゲームサーバに接続することにより、ユーザがネットワークを利用して各種のゲームを楽しむことができるようになっている。このようなゲーム環境は広い意味で「ネットワークゲーム環境」などと呼ばれるが、実際にユーザがネットワークを利用する形態は、幾つかのものがある。

【０００３】

第１の形態は、ユーザがオンラインでゲームを実行する形態である。即ち、ユーザは、ゲーム機を使用してゲームサーバとの通信を継続した状態でゲーム進行に要するデータをゲームサーバとの間で通信し、ゲームを実行する。この形態では、通常、ユーザがゲームサーバに接続してゲームを開始するたびに、ユーザの認証処理が要求される。つまり、ゲームサーバにアクセスしたユーザが、ユーザ登録などを完了した登録ユーザであるか、又は、実際にゲームサーバにアクセスしているユーザが登録ユーザ本人であるか、などをチェックする。このようなユーザ認証は、一般的にはユーザ登録時に発行されたユーザＩＤ及びパスワードをユーザがゲーム機に対して入力し、ゲームサーバへ送信することにより行われる。ゲームサーバは、受信したユーザＩＤ及びパスワードが登録ユーザのものであるかをチェックし、ユーザ認証を実行する。

【０００４】

一方、第２の形態では、ユーザはオンラインでゲームを実行するのではなく、ゲームプログラムの流通手段としてネットワークを利用する。つまり、ユーザはネットワークを介してゲームサーバへ接続し、所望のゲームを選択してそのゲー

ムプログラムを自分のゲーム機へダウンロードする。ダウンロードが完了すればゲームプログラム自体はユーザのゲーム機側に存在するので、原則としてユーザはゲームを実行するためゲームサーバへ接続する必要はなくなる。

【０００５】

【発明が解決しようとする課題】

ネットワークを利用したゲームにおいては、幾つかの問題がある。その１つはユーザの認証の問題である。上述ように第１の形態においては、ユーザ認証は一般的にユーザＩＤとパスワードの組み合わせによって行われる。しかし、ユーザＩＤとパスワードを利用したユーザ認証処理は、以下のような理由でセキュリティ面では非常に弱いと言わざるをえない。

【０００６】

まず、ユーザＩＤやパスワードは第三者による複製、偽造が容易である。ユーザＩＤやパスワードは単なる文字列であり、しかもユーザがゲーム機に対して手入力することを前提に作成されているため、せいぜい１０桁程度の長さであるのが普通である。よって、不正に他の登録ユーザになりすましてゲームを行おうとする者は、何通りもの文字列を推測して入力することにより、比較的容易に他人のユーザＩＤやパスワードを推測することができる。また、一旦他人に知られると、さらに他の者へと急速に頒布される危険性もある。１つのユーザＩＤ及びパスワードを複数人が同時に使用できるので、ユーザＩＤやパスワードが広まってしまうと、誰もがそれを利用して不正にゲームを行うことができてしまう。

【０００７】

ユーザＩＤやパスワードの桁数を増やせば推測は困難となるのであるが、一般的にユーザＩＤやパスワードは人間が記憶しておき手入力するものであるから、入力間違いやパスワードの紛失（忘れる）が起きやすい。よって、結局それほど長いユーザＩＤやパスワードを使用することはできず、安全性の面では自ずと限界がある。

【０００８】

さらには、ユーザがゲーム機からゲームサーバへ送信したユーザＩＤやパスワードを、ネットワーク上の通信途中において傍受して取得したり、ダミーの認証

サーバを構成してゲーム機に対してあたかもユーザ認証が成功したかのように認証結果情報を送信して、不正にゲームを実行可能とすることも可能である。

【０００９】

一方、上述の第２の形態のように、ネットワークをゲームプログラムの流通手段として使用する場合には、ユーザに対するゲームの使用期限管理の問題がある。通常、ユーザがダウンロードするゲームプログラムは有料であり、使用料の支払いを条件に一定期間（無期限の場合を含む）ゲームの使用を許可する方式が一般的である。このような場合に、使用期間を管理するために行われる１つの方法は、ユーザがゲームを始める際に、まずゲームサーバへ接続して認証処理を行うことを義務づける方法である。ゲームサーバは、ユーザから接続があると、そのユーザのゲームの使用期限をチェックし、使用期限内である場合にはゲームの実行を許可する情報をゲーム機へ送信してゲームを実行可能とする。

【００１０】

しかし、ゲームを開始するたびにゲームサーバへの接続が要求されるというのは、ユーザにとっては煩雑であり、また、通信コストもかかる。よって、使用料の支払いが完了すれば、ユーザにゲームサーバへの接続を行わせることなく、ゲーム機側のみで利用可能な期間を管理することが望まれる。

【００１１】

本発明の目的は、以上の点に鑑みてなされたものであり、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、ユーザの認証や使用期限の管理を確実に行い、ユーザが安全かつ快適にゲームを行うことを可能とすることにある。

【００１２】

【課題を解決するための手段】

本発明の１つの観点では、ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部

と、受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備える。

【００１３】

上記のハードウェアは、端末装置に取り付けられることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザＩＤ、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

【００１４】

暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止で

きる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与えられ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

【００１５】

なお、暗号化処理部、送信部、受信部及び復号化処理部は、集積回路として構成することができ、これにより各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる。

【００１６】

また、記憶部は取り外し可能に構成することができる。これにより、ハードウェアの他の部分を故障その他の理由により交換する必要が生じた場合に、認証情報を記憶した記憶部のみは交換せず、そのまま使用し続けることができる。よって、認証情報を変更する必要なく、ハードウェアの交換やバージョンアップなどに対応することができる。

【００１７】

上記の認証処理ハードウェアの一態様では、前記復号化処理部は、１つの前記暗号鍵を利用した復号化処理を１回に限り行う。これにより、サーバ装置から送信された暗号化済みの認証結果情報をネットワーク上で取得し、ダミーの認証サーバなどを利用して端末装置へ送信した場合でも、その暗号化済み認証結果情報に対応する暗号鍵は既に使用済みとなっているため、認証結果情報の復号化は行えない。これにより、ダミーの認証サーバなどを利用した不正な認証処理を防止することができる。

【００１８】

上記の認証処理ハードウェアの他の一態様は、前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備える。これにより、認証結果に応じて端末装置を動作させることができる。

【００１９】

本発明の他の観点では、ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアと、を備える認証処理システムが提供される。前記サーバ装置は、前記ハードウェアからの認証

要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する暗号鍵送信部と、前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備える。また、前記ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備える。また、前記端末装置は、前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備える。

【００２０】

上記の認証処理システムによれば、ハードウェアは、端末装置に取り付けられることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザＩＤ、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

【００２１】

暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号

鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止できる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与えられ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

【００２２】

本発明の他の観点では、端末装置に取り付けられ、前記端末装置の利用可否の管理処理を実行する利用管理ハードウェアは、前記端末装置の利用可否を示す利用可否情報を記憶する記憶部と、前記端末装置から、動作要求を受信する受信部と、前記利用可否情報に基づいて前記端末装置の利用可否を判定する判定部と、前記端末装置の利用が可能であると前記判定部が判定したときに、前記端末装置を動作可能とする制御部と、を備える。

【００２３】

上記の利用管理ハードウェアは、端末装置の利用可否の管理を行う。記憶部内には、端末装置の利用可否情報が記憶されている。端末装置から動作要求がなされると、利用管理ハードウェアは利用可否情報に基づいて、端末装置の利用が可能であるか否かを判定する。利用可否情報は、端末装置の使用期限や使用可能日数、使用可能時間数などの時間ベースの情報とすることもできるし、プリペイド式のカウント値などのポイント情報とすることもできるし、端末装置を使用するための何らかの特殊な契約や権限に基づく情報とすることもできる。なお、利用可否情報は、これらの例を含めて、端末装置の利用可否の判定に用いることができる各種の情報を含むものとする。例えば、利用可否情報が利用期限の日時や利用可能総時間数などで規定されている場合には、判定部を時計機能により構成することができ、利用可否情報がプリペイド式のカウント値などで規定されている

場合には、判定部をカウンタ機能により構成することができる。制御部は、判定部により利用可能と判定された場合に端末装置の動作を許可する。これにより、端末装置の利用可否の管理を容易に行うことができる。

【００２４】

なお、受信部、判定部及び制御部は、集積回路として構成することができる。これにより、各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる

【００２５】

【発明の実施の形態】

以下、図面を参照して本発明の好適な実施の形態について説明する。

【００２６】

［ネットワークゲーム環境］

図１に本発明を適用したネットワークゲーム環境の概略構成を示す。図１において、ゲームの提供者が運営するゲームサーバ５と、ユーザが使用するゲーム機１６とがネットワーク３を介して通信可能に構成されている。ネットワーク３の１つの好適な例はインターネットであるが、それ以外のネットワークであってもよい。また、ネットワーク３がインターネットである場合には、ユーザのゲーム機１６とネットワーク３との間にはインターネットサービスプロバイダ（ＩＳＰ）その他が介在することとなるが、ここではそれらの説明は省略する。

【００２７】

ゲーム機１６は、好適にはユーザが家庭で使用するゲーム機であるが、遊技場などに設置される業務用のゲーム機であっても構わない。なお、図１においては説明の便宜上、１台のゲーム機１６のみが図示されているが、実際には多数のユーザが所有する多数のゲーム機１６が同様にネットワーク３を介してゲームサーバ５と通信可能に構成される。

【００２８】

ゲームサーバ５は、ユーザに対してネットワーク３を通じてゲームを提供する。ゲーム提供の１つの形態は、前述のようにゲーム機１６とゲームサーバ５との間で通信することにより、ユーザがオンラインでゲームを実行するものである。

この場合、ゲームサーバ５とユーザとが１対１でゲームを実行する場合もあるし、ゲームサーバ５の管理下で複数のユーザが各々ゲーム機１６を操作して同時に同一のゲームを実行する場合もある。いずれの場合にも、ユーザは、ゲームを開始するときにゲームサーバ５へ接続し、ユーザ認証処理を行うことになる。

【００２９】

一方、前述の第２の形態では、ユーザはネットワークを１つの流通手段として利用し、ゲームサーバ５から所望のゲームプログラムをダウンロードする。ゲームプログラムは通常は有料であり、ユーザはゲームプログラム使用料を、何らかの方法でゲームサーバ５を運営する会社に対して支払う。ゲームプログラム使用料の支払いにより、ユーザは所定期間のゲーム使用権を取得することになる。ゲームサーバ５は、ユーザによるゲームプログラム使用料の支払いを条件に、ネットワーク３を通じてゲームプログラムをユーザのゲーム機１６へダウンロードさせる。その後は、ユーザは、既に支払ったゲームプログラム使用権利の範囲内（例えば、所定期間内）では、ダウンロードしたゲームプログラムを自由に使用することができる。よって、ゲームサーバ５を運営するゲーム提供者は、使用期限が経過したときにユーザによる当該プログラムの使用を禁止するための方策を採る必要がある。以下、この処理を「使用期限管理」と呼ぶことにする。

【００３０】

図１に示すように、本発明のネットワークゲーム環境では、セキュリティモジュール３０が使用される。セキュリティモジュール３０は、上述のユーザ認証や使用期限管理を行うために使用される専用モジュールであり、ゲーム１６機に取り付けて使用される。物理的にはセキュリティモジュール３０は内部構造がわからないように製作されたハードウェア装置であり、ゲーム機１６の所定のコネクタなどに取り付けられる。ゲーム機１６は、セキュリティモジュール３０が取り付けられた状態でなければ、ゲームサーバ５を利用したネットワークゲームを実行できないように構成される。なお、ゲームサーバ５とは無関係の市販ゲームソフトなどを使用する場合には、ゲーム機１６はセキュリティモジュール３０なしでも動作するように構成することができる。本発明では、セキュリティモジュール３０を使用することにより、前述のユーザ認証処理や使用期限管理などを、簡

単かつ確実に実行することが可能となる。

【００３１】

［ゲーム機の構成］

次に、図１に示すゲーム機の構成について説明する。図２はゲーム機１６を含むゲーム装置２０のブロック図である。

【００３２】

このゲーム装置２０は、モニタ９、スピーカ１０ａ及び１０ｂ、コントローラ１２、補助記憶装置１３、ＤＶＤ－ＲＯＭ１５、ゲーム機１６で構成される。モニタ９には家庭用のテレビ受像機が、スピーカ１０ａ及び１０ｂにはそのテレビ受像機の内蔵スピーカが一般に使用される。スピーカは、右チャンネルスピーカ１０ａ及び左チャンネルスピーカ１０ｂの２チャンネルを有する。コントローラ１２は入力装置として機能するものであり、そこにはプレイヤーによる操作を受け付ける操作部材が設けられる。補助記憶装置１３は、ゲーム進行状況などに関連するデータを記憶するための記憶媒体であり、例えば半導体メモリなどを使用することができる。

【００３３】

ゲーム機１６は、マイクロプロセッサを主体として構成されたＣＰＵ１と、そのＣＰＵ１に対する主記憶装置としてのＲＯＭ２及びＲＡＭ３と、画像処理及び音声処理用のグラフィックスプロセッシングユニット（ＧＰＵ）４及びサウンドプロセッシングユニット（ＳＰＵ）６と、それらのユニットに対するバッファ５、７と、ＤＶＤ－ＲＯＭ読取装置８と、インターフェース１７と、コネクタ１８と、ハードディスク（ＨＤＤ）１９と、を有している。

【００３４】

ＲＯＭ２には、ゲーム機の動作制御に必要なプログラムとしてのオペレーティングシステムが格納されている。ＲＡＭ３には記憶媒体としてのＤＶＤ－ＲＯＭ１５から読み取ったゲーム用のプログラムやデータが必要に応じて書き込まれる。

【００３５】

ＧＰＵ４はＣＰＵ１から画像データを受け取ってフレームバッファ５上にゲー

ム画面を描画するとともに、その描画された画像のデータを所定のビデオ再生信号に変換して所定のタイミングでモニタ９に出力する。ＳＰＵ６は、ＤＶＤ－ＲＯＭ１５から読み出されてサウンドバッファ７に記録された音声、楽音等のゲーム音データ等を再生してスピーカから出力させる。

【００３６】

ＤＶＤ－ＲＯＭ読取装置８は、ＣＰＵ１からの指示に従ってＤＶＤ－ＲＯＭ１５上に記録されたプログラムやデータを読み取り、その読み取った内容に対応した信号を出力する。ＨＤＤ１９には、ゲームサーバ５からダウンロードしたゲームプログラムなどが格納される。

【００３７】

コネクタ１８は、セキュリティモジュール３０をゲーム機１６に取り付ける際に使用され、セキュリティモジュール３０側のコネクタと接続される。コネクタ１８は、インターフェース１７を介してバス１４と接続されている。

【００３８】

ＣＰＵ１にはバス１４を介して通信制御デバイス１１が接続され、通信制御デバイス１１にはコントローラ１２及び補助記憶装置１３がそれぞれ着脱自在に接続される。通信制御デバイス１１は一定周期（例えば１／６０秒）でコントローラ１２の操作部材の操作状態を走査し、その走査結果に対応した信号をＣＰＵ１に出力する。ＣＰＵ１はその信号に基づいてコントローラ１２の操作状態を判別する。また、通信制御デバイス１１は、ネットワーク３を介してゲームサーバ５と必要な通信を行うために機能する。

【００３９】

ゲーム機１６は、記憶媒体としてのＤＶＤ－ＲＯＭ１５に記録されたゲームプログラムに従って所定のゲームを実行することができる。また、ネットワーク３をゲームプログラムのダウンロード手段として使用する場合には、ゲームサーバ５からダウンロードしたゲームプログラムは、ゲーム機１６内部のＨＤＤ１９に保存される。よって、ゲーム機１６は、ＤＶＤ－ＲＯＭ１５に記録されたゲームプログラムの代わりに、ゲームサーバ５からダウンロードし、ＨＤＤ１９に格納したゲームプログラムに従ってゲームを実行することもできる。

【００４０】

ネットワークゲーム実行時には、ＣＰＵ１は、ＤＶＤ－ＲＯＭ１５に記録されたゲームプログラム又はゲームサーバ５からダウンロードしたゲームプログラムを実行する。そして、その過程で発生する、ゲーム機１６におけるユーザのプレイ状況データを、通信制御デバイス１１及びネットワーク３を介してゲームサーバ５に送信する。また、必要に応じて、サーバが生成するゲーム状況データや、ネットワーク上で同時にゲームをプレイしている他のユーザのプレイ状況データをゲームサーバ５から受信する。こうして、ゲーム機１６はオンラインゲームを進行させる。

【００４１】

［セキュリティモジュール］

次に、セキュリティモジュールについて説明する。図３にセキュリティモジュール３０の概略構成を示す。図３に示すように、セキュリティモジュール３０は、大別すると、Ｉ／Ｆユニット３０ａ、処理ユニット３０ｂ及び記憶ユニット３０ｃにより構成される。セキュリティモジュール３０内部の各ユニットはメモリ、フラッシュ、及び集積回路などを含むハードウェアユニットとして、内部に記憶した情報に対する外部からのアクセスが不能となるように構成される。これは、例えばゲーム機１６への取付用コネクタ４０などのゲーム機１６との入出力手段を除き、外部からの入出力手段や入出力端子を設けないなどの方法で実現できる。

【００４２】

Ｉ／Ｆユニット３０は、ゲーム機１６との接続のためのユニットであり、Ｉ／Ｆ３１と、コネクタ４０とを備える。コネクタ４０は、図２に示すゲーム機１６のコネクタ１８と接続される。Ｉ／Ｆ３１は、セキュリティモジュール３０内のデータとゲーム機１６側のデータとの間のインターフェース処理を行う。

【００４３】

記憶ユニット３０ｃは、認証情報記憶部３８と、不揮発性メモリ３９とを備える。認証情報記憶部３８は、ユーザＩＤ、パスワードなどの認証情報を記憶する。一方、不揮発性メモリ３９は、認証情報以外の各種情報を記憶する。具体的に

は、ユーザが特定の有料ゲームプログラムをダウンロードした場合の使用期限情報を記憶する。使用期限情報は、例えば「○年○月○日」のように終了日時で記憶してもよく、何百時間というように時間で記憶しても良い。

【００４４】

処理ユニット３０ｂは、ＣＰＵなどにより構成され、時計機能３３、暗号化機能３４、復号化機能３５及び通信機能３６を備える。ＣＰＵが予め用意された各プログラムを実行することにより、各機能が実現される。時計機能３３は、セキュリティモジュール独自の内部時計であり、基本的に外部からの調整などができないように構成される。

【００４５】

暗号化機能３４は、ユーザ認証処理において、認証情報記憶部３８に記憶されている認証情報（ユーザＩＤ、パスワードなど）を所定の暗号鍵を利用して暗号化する処理を行う。暗号化された認証情報は、ユーザ認証処理においてゲームサーバ５へ送られる。復号化機能３５は、ゲームサーバ５から送信された暗号化済み情報を復号化する。また、通信機能３６は、暗号化されたユーザ認証情報やゲームサーバから送信される情報などの通信処理を実行する。

【００４６】

［ユーザ認証処理］

次に、ユーザ認証処理について説明する。ユーザ認証処理は、ユーザがゲーム装置２０を使用してゲームサーバ５に接続し、ネットワークゲームを開始する際に実行される処理であり、当該ユーザがゲームをプレイすることができる登録ユーザであるか否かを判別するための処理である。

【００４７】

通常、ユーザ認証処理においては、ユーザ自身がユーザＩＤやパスワードなどの認証情報をゲーム装置２０対して入力し、それがネットワーク３を介してゲームサーバ５へ送信される。これに対し、本発明では、ユーザＩＤ及びパスワードなどの認証情報はセキュリティユニット３０の認証情報記憶部３８内に記憶されており、外部からアクセスすることはできない。即ち、認証情報はハードウェアの形態でセキュリティモジュール３０に実装されているので、複製が困難であり

、また、記憶されている認証情報をセキュリティモジュール３０から外部へ取り出すことも困難である。また、ユーザ自身も、実際に記憶されている認証情報を知らなくても、セキュリティモジュール３０を所持していれば済むので、認証情報自体が漏洩したり、不正に流通することが防止できる。また、万が一第三者が認証情報を知得することができたとしても、その認証情報をユーザ認証処理において入力する術がない。また、セキュリティモジュール３０は物理的な１つの存在であるため、複数の人間が同時に使用することはできない。さらに、人間がユーザＩＤやパスワードを手入力する場合と異なり、入力ミスも発生しないし、ユーザＩＤやパスワードの桁数をかなり長くすることができるので安全性をより高めることができる。

【００４８】

次に、セキュリティモジュール３０とゲームサーバ５との間で行われるユーザ認証処理について説明する。なお、セキュリティモジュール３０から入出力されるデータは、まずゲーム機１６に入力されることになるが、ゲーム機１６内を単に通過するだけであり、ゲーム機１６はそのデータに対して特に処理を行わない。つまり、ユーザ認証処理は実質的にセキュリティモジュール３０とゲームサーバ５との間で実行されることになる。

【００４９】

ユーザ認証処理においては、セキュリティモジュール３０内に記憶されているユーザの認証情報（ユーザＩＤ、パスワードなど）を、ネットワーク３を介してゲームサーバ５へ正しく送信することが要求される。また、その際に、第三者が送信されたデータをネットワーク上で不正に傍受し、認証情報を知得することを防止しなければならない。このため、本実施形態では、セキュリティモジュール３０は、暗号化機能３４により認証情報を暗号化してからゲームサーバ５へ送出する。これにより、第三者がネットワーク３上で送信されたデータを取得し、それから認証情報を解析することが防止できる。

【００５０】

また、ゲームサーバ５上で登録ユーザに対するユーザ認証が正しく完了すると、ゲームサーバ５はその旨の通知、つまり、当該ユーザのゲーム機１６にゲーム

の実行を許可するための許可情報をセキュリティモジュール３０へ送信することになる。セキュリティモジュール３０は、この許可情報を受け取ると、ゲーム機１６を制御してゲームの実行を可能とする。ゲームサーバ５はこの許可情報も暗号化して送出する。

【００５１】

一方、ユーザのゲーム使用期間が終了した場合、当該ユーザは同様の手順でゲームサーバ５へユーザ認証を行っても、ゲームサーバ５側は当該ユーザのゲーム使用期間が終了したことを知っているので、ユーザ認証は不成功に終わる。

【００５２】

そのような場合、当該ユーザは、ゲーム使用期間満了前に正しくユーザ認証処理が行われた際にゲームサーバ５からセキュリティモジュール３０へ送信された許可情報をネットワーク３上で取得しておき、ゲーム使用期間の終了後にダミーサーバ（偽りのゲームサーバとして機能する）を用意して、同じ許可情報をダミーサーバから自己のゲーム機１６へ送信しようとすることがありうる。こうすると、ゲーム機１６は、ダミーサーバからの許可情報をゲームサーバ５からの許可情報であると誤認し、ゲームを実行してしまう可能性がある。

【００５３】

このような不正なユーザ認証を防止するために、本実施形態では、ゲームサーバ５からセキュリティモジュール３０へ送信される許可情報（暗号化済み）を１回限り有効とする。即ち、１つの許可情報は、セキュリティモジュール３０上において一回のみ有効であるとする。これは、例えばセキュリティモジュール３０内に、過去にゲームサーバ５から受信した許可情報の履歴を保存しておき、過去に使用された許可情報と同一の許可情報を再度受け取っても、その許可情報を無効とし、ゲームの実行を許可しないようにすることにより実現することができる。

【００５４】

また、許可情報を１回限り有効とする代わりに、許可情報を暗号化する鍵を１回限り有効とする方法もある。即ち、ゲームサーバ５は、特定の暗号鍵を使用して許可情報を暗号化し、セキュリティモジュール３０へ送信する。セキュリティ

モジュール３０は、その暗号鍵をゲームサーバ５から取得しており、当該暗号鍵を使用して許可情報を復号化し、ゲームを実行可能とする。ここで、セキュリティモジュール３０内では、一度使用された暗号鍵はその後の許可情報の復号化処理には使用できないように構成しておく。こうすれば、前述のダミーサーバから過去に使用した暗号鍵で暗号化された許可情報をゲーム機１６に再度送って不正にゲームを実行しようとした場合でも、その暗号鍵は既に過去に使用履歴があり、再度使用することはできないので、セキュリティモジュール３０は許可情報を得ることができない。これにより、使用期間経過後などの不正なゲーム実行を防止することができる。

【００５５】

次に、ユーザ認証処理の具体例について図４を参照して説明する。図４は、ユーザ認証処理のフローチャートである。まず、セキュリティモジュール３０は、ゲームサーバ５へ接続し、ユーザ認証を行う旨を要求する（ステップＳ１）。ゲームサーバ５は、これに対して、所定の暗号鍵を作成し、セキュリティモジュール３０へ送信する（ステップＳ２）。なお、暗号鍵は、セキュリティモジュール３０とゲームサーバ５との間で認証情報や許可情報を送受信する際の暗号化及び復号化に使用される鍵であり、例えば乱数などとすることもできる。

【００５６】

セキュリティモジュール３０は、暗号鍵を受信すると、認証情報記憶部３８から認証情報を取得し、これを暗号鍵で暗号化することにより暗号化した認証情報を作成してゲームサーバ５へ送信する（ステップＳ３）。認証情報は、例えばユーザＩＤ、パスワードなどを含む。ゲームサーバ５は、暗号化した認証情報を受信し、暗号鍵を使用して復号化することにより、認証情報を取得する（ステップＳ４）。そして、ゲームサーバ５は、認証情報が登録ユーザのものであるか否かを判定する（ステップＳ５）。これは、例えば登録ユーザについてのユーザ情報を記憶したデータベースなどを参照して、受信した認証情報が正規な登録ユーザのものであるか否かを判定することにより行われる。

【００５７】

認証情報が正規な登録ユーザのものであった場合（ステップＳ５；Yes）、ゲ

ームサーバ５はゲーム実行許可情報を生成し、これを暗号鍵で暗号化して暗号化済み許可情報を作成する（ステップＳ６）。一方、認証情報が正規な登録ユーザのものでなかった場合（ステップＳ５：No）、ゲームサーバ５は所定のエラー処理を行い、ダミーデータを作成する（ステップＳ７）。ここで、ダミーデータは、不正な目的によりデータの解析が行われることを防止するために生成されるものであり、例えば全く無意味なデータとすることができる。そして、ゲームサーバ５は、ステップＳ６で生成された暗号化済み許可情報又はステップＳ７で生成されたダミーデータを、認証結果情報としてセキュリティモジュール３０へ送信する（ステップＳ８）。

【００５８】

セキュリティモジュール３０は、認証結果情報を受信すると、暗号鍵でこれを復号化し（ステップＳ９）、ゲーム実行が許可されたか否かを判定する（ステップＳ１０）。認証結果情報が暗号化済み許可情報である場合、ステップＳ９の復号化処理により、暗号化が解除された許可情報が得られる。よって、セキュリティモジュール３０は、ゲーム装置２０に対してゲーム実行を許可し、ゲームを実行させる（ステップＳ１１）。一方、認証結果情報がダミーデータである場合、ステップＳ９の復号化は正しく行うことができないので、セキュリティモジュール３０はゲームの実行が許可されていないと判断し、ゲーム装置２０に対してゲームの実行許可を与えない（ステップＳ１２）。

【００５９】

以上のようにして、暗号鍵を使用して暗号化した認証情報及び許可情報を通信することにより、ユーザ認証がなされる。ゲームサーバ５は、セキュリティモジュール３０からユーザ認証の要求を受けるたびに、新しい暗号鍵を作成し、セキュリティモジュール３０へ送信する。従って、ステップＳ６で生成される許可情報は必ず新しい暗号鍵により暗号化されていることになり、セキュリティモジュール３０は新しい暗号鍵を有する正当な登録ユーザでなければゲーム実行を可能とする許可情報を取得することができない。

【００６０】

また、セキュリティモジュール３０は、一度ゲームサーバから受信した暗号鍵

を１回限り使用し、繰り返し使用しないこととする。これは、例えば、ユーザ認証要求を行うたびに、その後のステップＳ３でゲームサーバ５から受信した暗号鍵のみを使用するようにプログラムを構成するとか、一度ステップＳ９の復号化処理で使用した暗号鍵を消去するなど、いくつかの方法で実現することができる。

【００６１】

この方法によれば、前述のダミーサーバを利用した不正な認証処理も不成功とさせることができる。例えばあるユーザがプログラム使用期限の終了などにより正当にゲームを実行できなくなった状態で、前述のダミーサーバを用意し、過去にゲームサーバ５から送信された認証結果情報を偽りの認証結果情報としてダミーサーバからセキュリティモジュール３０に送信したとする。セキュリティモジュール３０はステップＳ９で認証結果情報を復号化するが、その認証結果情報を正しく復号化できる暗号鍵は過去に既に使用済みであり、セキュリティモジュール３０はその暗号鍵を１回のみ使用することとしているので、当該偽りの認証結果情報に基づいてセキュリティモジュール３０がゲーム実行許可を発することはない。よって、ダミーサーバを利用する不正な認証処理を無力化することができる。

【００６２】

なお、暗号化処理は一般的には特定の関数による演算処理であり、暗号鍵は当該関数の演算処理に使用するパラメータを示すデータとすることができる。

【００６３】

［使用期限管理］

次に、使用期限管理について説明する。使用期限管理とは、事前にゲーム使用料を支払ってゲームの使用権を得たユーザに対して、使用期限を管理し、使用期間経過後はゲームの使用を禁止するための処理である。このような使用期限管理は、ゲーム使用権を得た後でも、ユーザに対して常にゲーム開始前にゲームサーバ５へ接続してユーザ認証を行うことを義務付ければ、ゲームサーバ側で容易に行うことができる。しかし、正当な使用期間内であるにも拘わらず、ゲーム開始時にいちいちゲームサーバへ接続して認証処理を行うことは、ユーザにとっては

煩雑であったり、不快であったりする。また、ゲームサーバへ接続することにより、通信コストが発生し、ユーザはこれを負担する必要がある。よって、一度ゲームプログラム使用料を支払った後は、ゲームサーバへ接続する必要なく、ゲーム機側のみで使用期限の管理ができることが望ましい。本発明では、セキュリティモジュール３０によりこれを実現する。

【００６４】

具体的には、図３に示すセキュリティモジュール３０の不揮発性メモリ３９内に、使用期限情報が格納される。使用期限情報は、例えば何年何月何日まで使用可能であるという日時の情報、又は、合計何時間使用可能であるなどの時間情報などの形態で記憶することができる。

【００６５】

また、セキュリティモジュール３０内部の時計機能３３は、基本的に外部からの調整ができないように構成される。よって、ユーザがセキュリティモジュール３０内の時計機能３３にアクセスし、時刻を調整、変更することはできない。通常、ゲーム機１６内にも時計機能は内蔵されているが、これはユーザにより容易に変更可能に構成されている。よって、ゲーム機１６内の時計機能を利用して使用期限を管理するのでは、ユーザによる不正な時刻変更が容易に行われてしまう。この点、本発明のセキュリティモジュール３０によれば、内部の時計機能３３は外部からは変更不能であるので、使用期限を正しく管理することができる。

【００６６】

使用期限管理処理の一例を図５を参照して説明する。図５は、使用期限管理処理のフローチャートである。まず、ユーザが特定のゲームを実行すべくゲーム機１６を操作すると、ゲーム機１６はセキュリティモジュール３０に対してゲーム実行要求を行う（ステップＳ３０）。セキュリティモジュール３０は、ゲーム実行要求を受け取ると、まず不揮発性メモリ３９から使用期限情報を取得し（ステップＳ３１）、次に時計機能３３を利用して使用期限内であるか否かを判定する（ステップＳ３２）。

【００６７】

使用期限を過ぎている場合（ステップＳ３３；No）、セキュリティモジュール

３０はゲーム機に対してゲーム実行を許可しない（ステップＳ３４）。一方、使用期限内である場合（ステップＳ３３；Yes）、セキュリティモジュール３０はゲーム機に対してゲーム実行許可を与える。よって、ユーザはゲームを実行することができる。

【００６８】

なお、上記の説明では使用期限管理を日時や時間情報により行う例を示したが、本発明における使用期限管理はそのような時間による管理には限定されない。例えば、使用期限をゲーム何回分などという使用回数として設定し、セキュリティモジュール３０内にカウンタ機能を設けて使用回数をカウントすることにより使用期限を管理することもできる。また、ユーザが複数のゲームを選択的にプレイできる環境では、使用可能なポイント数を予めセキュリティモジュール３０内に記憶し、ユーザがあるゲームをプレイすると、そのゲームに対応するポイント数だけセキュリティモジュール３０内に記憶されたポイント数を減算していくこともできる。この場合のポイント数は、ゲームをプレイするためのプリペイド方式の電子マネー的な意味を有することになる。なお、そのようにセキュリティモジュール内にカウンタ機能を設ける場合には、前述の時計機能と同様に外部からカウント値の調整やリセットなどが不能なようにカウンタ機能を構成する。

【００６９】

［変形例］

上記の実施例においては、セキュリティモジュール３０をゲーム機１６に取り付け、セキュリティモジュール３０とゲームサーバ５との間のデータ通信はゲーム機１６内を通過するように構成されていた。代わりに、図６に示すように、セキュリティモジュール３０がネットワーク３に接続され、ゲーム機１６へはセキュリティモジュール３０内を通過してデータが供給されるように構成することもできる。この場合、セキュリティモジュール３０によるユーザ認証の対象となるデータはセキュリティモジュール３０による処理後にゲーム機１６に送られる。一方、セキュリティモジュール３０の処理対象外のデータ（例えば無償のゲームプログラムのダウンロードなど）は、セキュリティモジュール３０内をそのまま通過してゲーム機１６へ送られる。

【００７０】

図３に示すように、セキュリティモジュール３０はＩ／Ｆユニット３０ａ、処理ユニット３０ｂ及び記憶ユニット３０ｃにより構成されている。ここで、セキュリティモジュール３０は、３つのユニットを一体的に構成することもできるが、記憶ユニット３０ｃのみを例えばカード型の記憶媒体などとして、他の２つのユニットから取り外し可能に構成することもできる。これには以下のようなメリットがある。３つのユニットが一体的に構成されていると、例えばＩ／Ｆユニット３０ａ及び処理ユニット３０ｂ内のいずれかの箇所が故障したような場合、３つのユニット全体として交換を行う必要がある。また、故障に限らず、セキュリティモジュール３０による処理が多機能化したような場合にも、セキュリティモジュール全体を交換する必要が生じる。しかし、記憶ユニット３０ｃはユーザの認証情報及びゲームの使用期限情報などの情報を記憶したユニットであるので、これを含めてセキュリティモジュール３０全体を交換してしまうと、記憶ユニット３０ｃ内に記憶されている認証情報やゲーム使用期限情報などを使用不可となってしまう。この点、記憶ユニット３０ｃのみを取り外し可能に構成しておけば、上記のような理由で他の２つのユニットを交換する必要が生じた場合でも、記憶ユニット３０ｃ内の認証情報などをそのまま引き継ぐことができる。

【００７１】

【発明の効果】

以上説明したように、本発明によれば、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、高いセキュリティを確保してユーザが安全かつ快適にゲームを行うことが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用したネットワークゲーム環境の概略構成を示すブロック図である。

【図２】

ゲーム装置の概略構成を示すブロック図である。

【図３】

セキュリティモジュールの内部構成を示す機能ブロック図である。

【図４】

ユーザ認証処理のフローチャートである。

【図５】

使用期限管理処理のフローチャートである。

【図６】

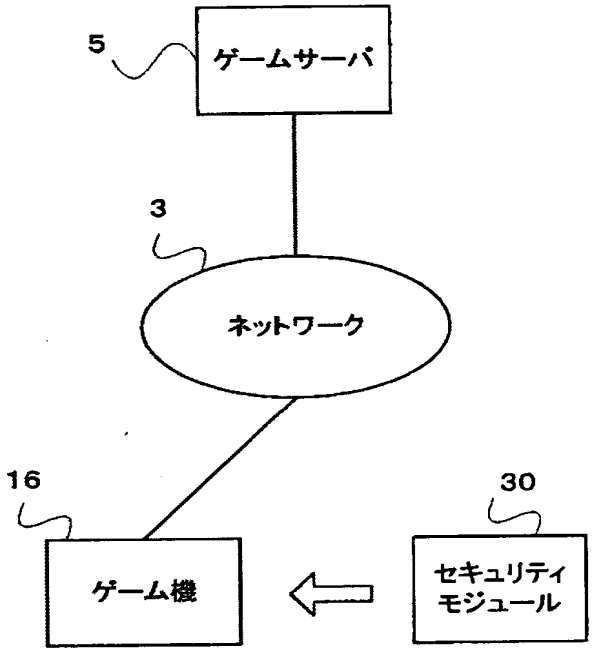
本発明の変形例によるゲーム機とセキュリティモジュールの構成を示すブロック図である。

【符号の説明】

１	ＣＰＵ
２	ＲＯＭ
３	ＲＡＭ
４	ＧＰＵ
５	フレームバッファ
６	ＳＰＵ
７	サウンドバッファ
８	ＤＶＤ－ＲＯＭ読取装置
９	モニタ
１１	通信制御デバイス
１２	コントローラ
１３	補助記憶装置
１４	バス
１５	ＤＶＤ－ＲＯＭ
１６	ゲーム機
２０	ゲーム装置
３０	セキュリティモジュール

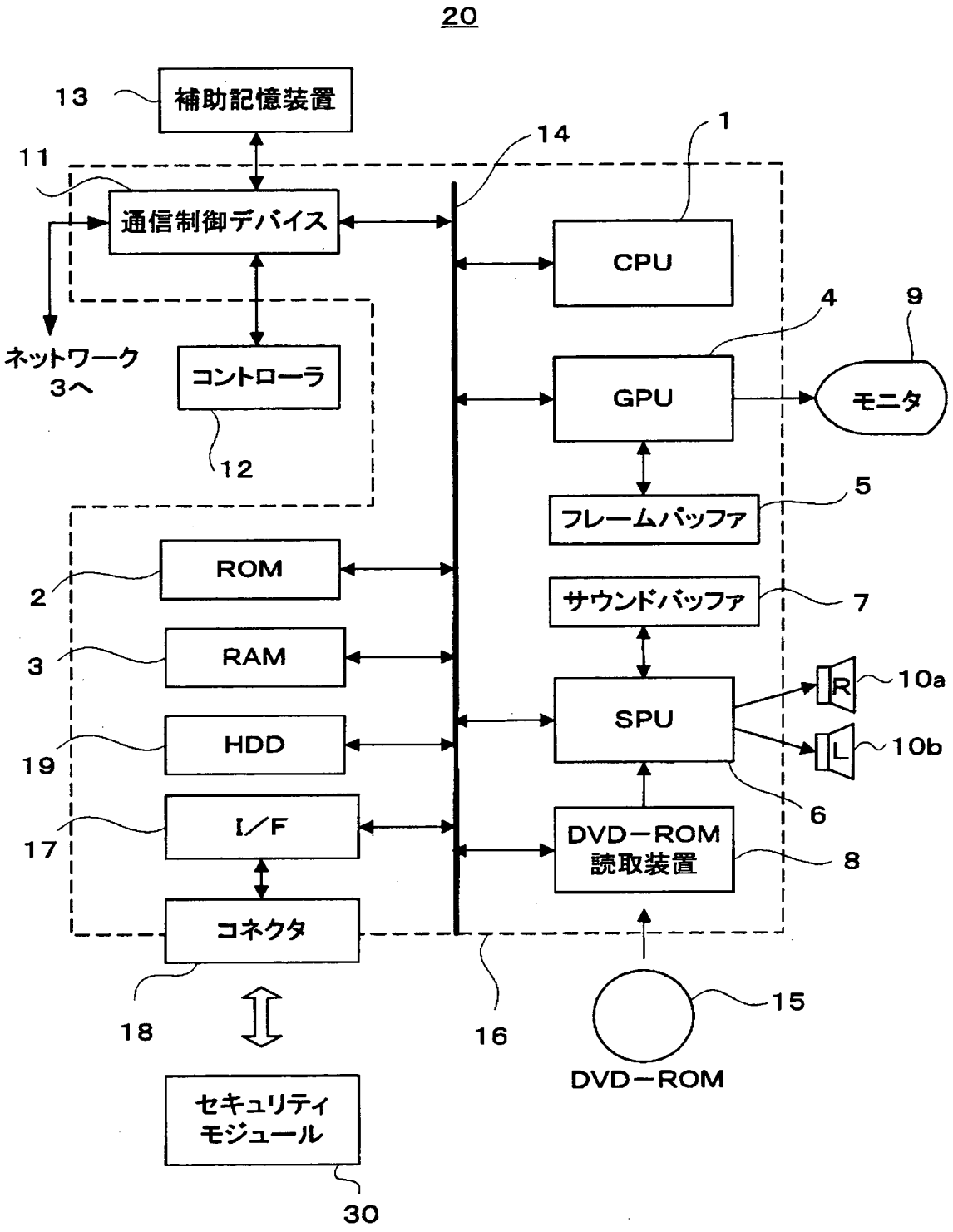
【書類名】　　図面

【図１】

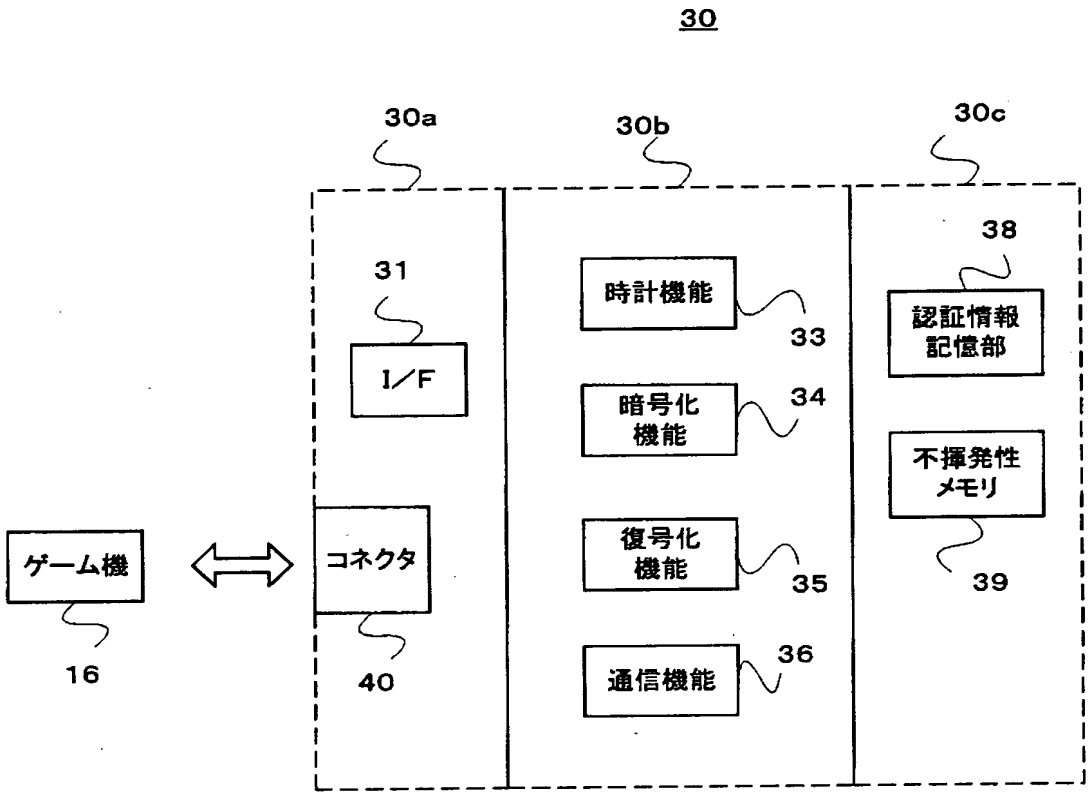


出証特２００３－３０５０２０６

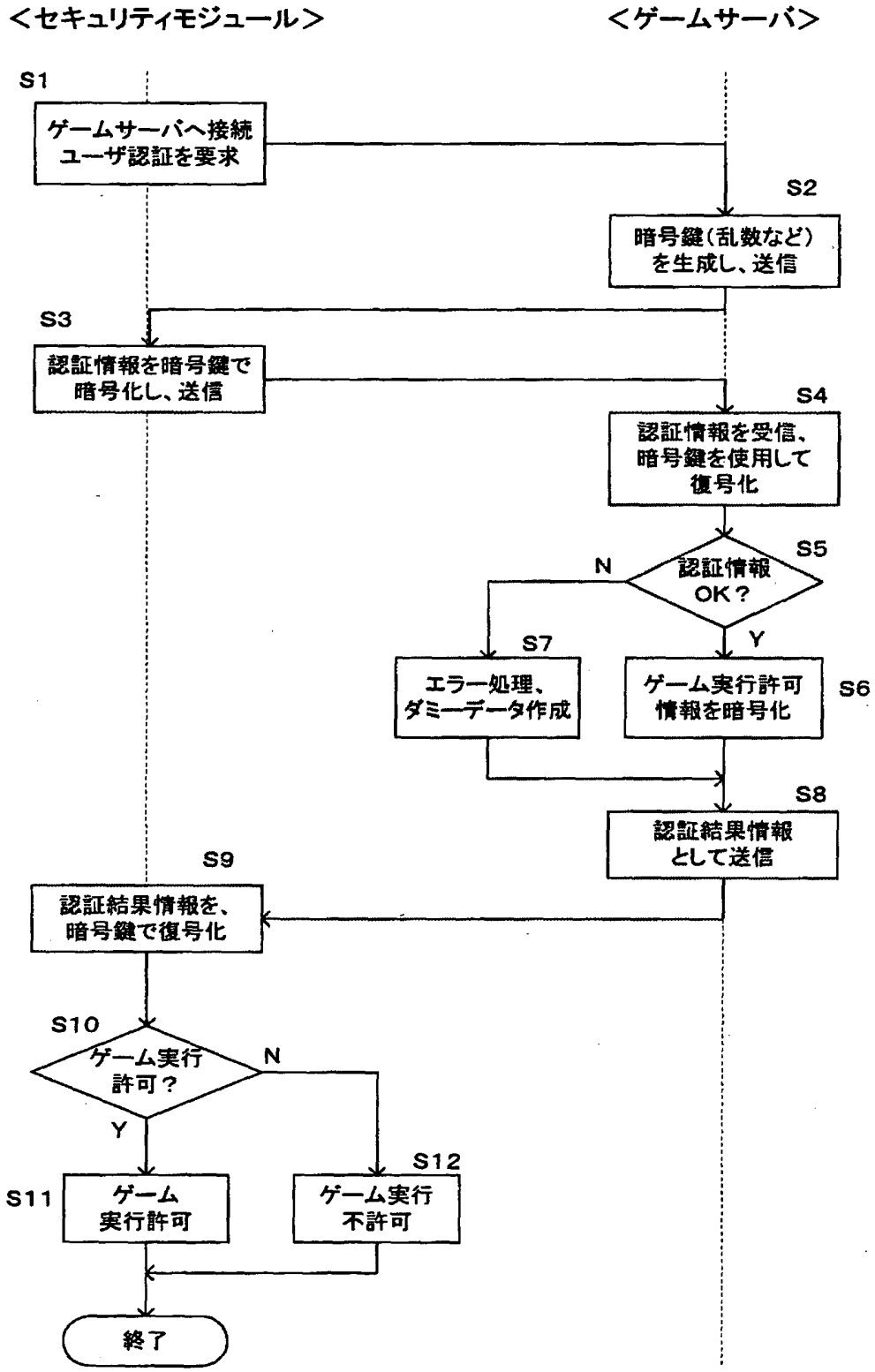
【図２】


20
13
補助記憶装置
11
通信制御デバイス
ネットワーク
3へ
コントローラ
12
14
1
CPU
4
9
GPU
モニタ
5
フレームバッファ
ROM
2
サウンドバッファ
7
RAM
3
R
10a
SPU
L
10b
HDD
19
6
I／F
17
DVD－ROM
読取装置
8
コネクタ
18
16
15
DVD－ROM
セキュリティ
モジュール
30

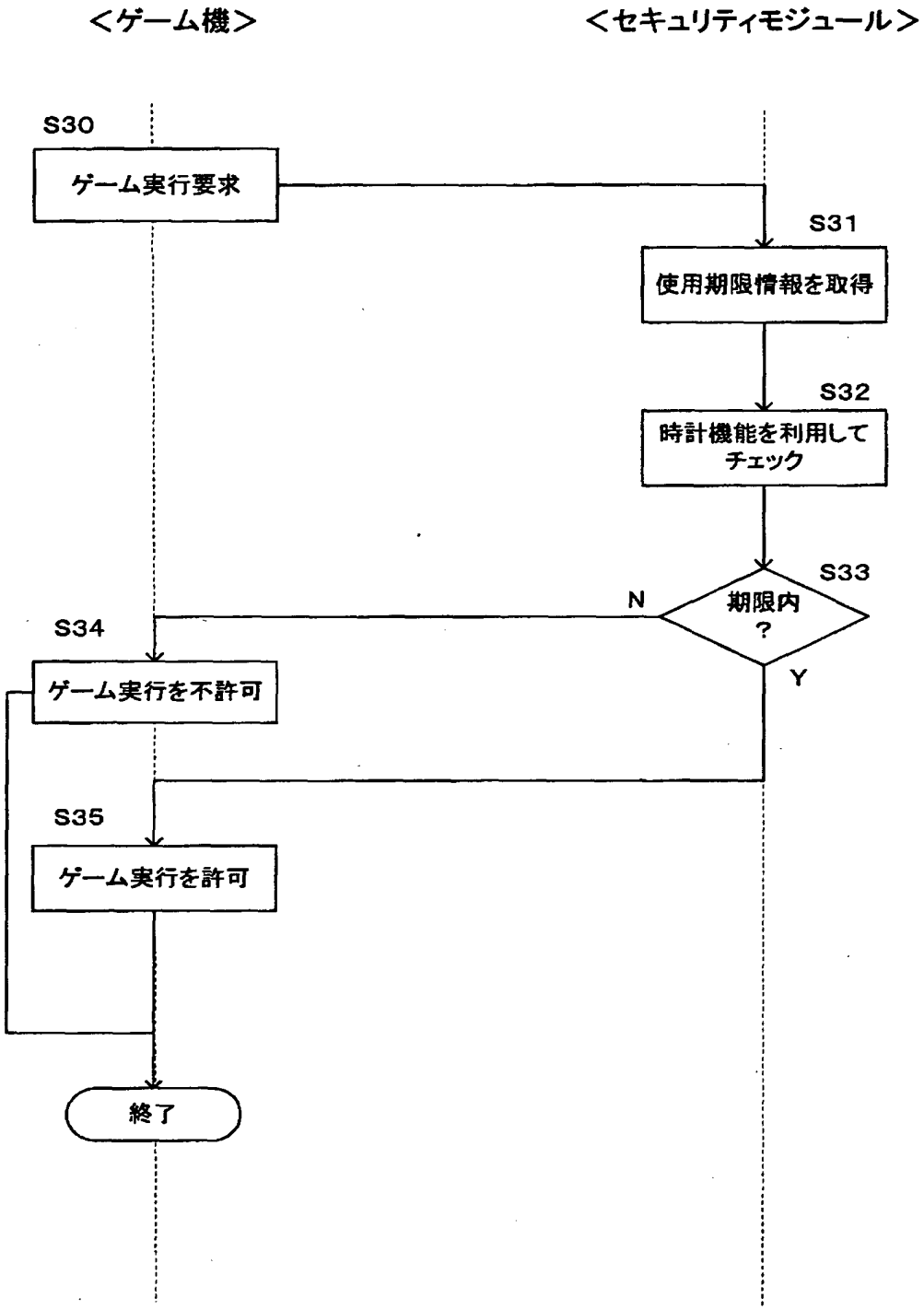
【図３】


30
30a
30b
30c
31
I/F
コネクタ
40
ゲーム機
16
時計機能
33
暗号化機能
34
復号化機能
35
通信機能
36
38
認証情報記憶部
不揮発性メモリ
39

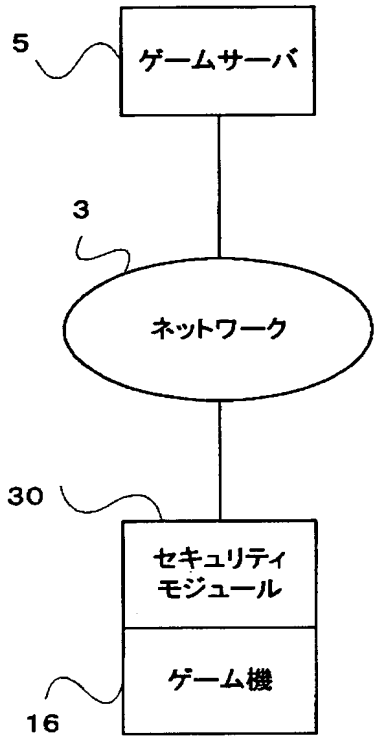
【図４】


<セキュリティモジュール>
<ゲームサーバ>
S1
ゲームサーバへ接続
ユーザ認証を要求
S2
暗号鍵(乱数など)
を生成し、送信
S3
認証情報を暗号鍵で
暗号化し、送信
S4
認証情報を受信、
暗号鍵を使用して
復号化
S5
認証情報
OK？
N
Y
S7
エラー処理、
ダミーデータ作成
S6
ゲーム実行許可
情報を暗号化
S8
認証結果情報
として送信
S9
認証結果情報を、
暗号鍵で復号化
S10
ゲーム実行
許可？
N
Y
S11
ゲーム
実行許可
S12
ゲーム実行
不許可
終了

【図５】


<ゲーム機>
<セキュリティモジュール>
S30
ゲーム実行要求
S31
使用期限情報を取得
S32
時計機能を利用して
チェック
S33
期限内
?
N
Y
S34
ゲーム実行を不許可
S35
ゲーム実行を許可
終了

【図６】



【書類名】　　要約書

【要約】

【課題】　ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、高いセキュリティを確保してユーザが安全かつ快適にゲームを行うことを可能とする認証処理ハードウェア及びシステムを提供する。

【解決手段】　認証処理ハードウェアは、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などに取り付けられ、ユーザの認証処理を実行する。認証処理ハードウェアは、ユーザの認証情報を記憶する記憶部と、サーバ装置から与えられた暗号鍵で認証情報を暗号化してサーバ装置へ送信する認証情報送信部と、サーバ装置から認証結果情報を受信する認証結果情報受信部と、認証結果情報を復号化する認証結果復号化処理部とを備える。認証情報は、例えばユーザＩＤ、パスワードなどを含むことができる。認証情報は、認証処理ハードウェア内部に記憶されており、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。よって、ユーザがユーザＩＤやパスワードを手入力するユーザ認証方法と比べて、安全性を大幅に改善することができる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００１０５６３７〕

１．変更年月日　　２００２年　８月２６日
［変更理由］　住所変更
住　所　　東京都千代田区丸の内２丁目４番１号
氏　名　　コナミ株式会社